РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

Список использованных источников:
1. Medvetz T. Think tanks as an emergent field. New York: Social Science Research Council, 2008. – 10 p. Эл. ресурс: http://www.ssrc.org/publications/view/A2A2BA10-B135-DE11-AFAC-001CC477EC70/. Доступно с января, 2014.
2. Rich A. Think Tanks, Public Policy и Expert of Expertise / A. Rich. Кембридж; Нью-Йорк: Кембриджский университет. Press, 2004. P. 13
3. Dixon P. Factories of Thought / P. Dixon. Москва: IST, 2004. P. 42.
4. McGann, J. G. Weaver, R. Аналитические центры и гражданские общества: катализаторы идей и действий. Нью-Брансуик, Нью-Джерси: издатели транзакций. 2000
5. Хоггинс Р.Л. Некоммерческие общественные исследовательские организации. Справочник по мозговым центрам в правительстве. Garland Publishing, Inc., Нью-Йорк и Лондон, 1993. P.16
6. Hauck J.C.R. What are “Think Tanks”? Revisiting the Dilemma of the Definition. São Paulo: Brazilian Political Science Review, 2017. - №11(2). Available at https://doi.org/10.1590/1981-3821201700020006
7. Gerasymchuk S. Think-tanks – the problems of definition and the way to solve them. Think Tanks Development and Research Initiative “think twice UA”, February 23, 2017. Available at http://thinktwiceua.org/wp-content/uploads/Think-tank-definition-article-SG-2.pdf
8. Weaver K.R., McGann J.G. (eds). Think-Tanks and Civil Societies. Catalysts for Ideas and Action. Piscataway, NJ: Transaction, 2000.
9. Pautz H. Think-tanks, social democracy and social policy. Palgrave Macmillan, 2014.
10. McGann. Think Tanks and the transnationlization of foreign policy // [Электронный ресурс]. URL: https://globalnetplatform.org/system/files/1/Think%20Tanks%20and%20the%20Transnationalization%20of%20Foreign%20Policy.pdf p. 2-3
11. Boucher, Stephen, et al., Europe and its think tanks; a promise to be fulfilled. An analysis of think tanks specialized in European policy issues in the enlarged European Union, Studies and Research No 35. October. Paris: Notre Europe, 2004. 154 p., p.2-3

УДК 327

КИБЕРДИПЛОМАТИЯ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Омарова Динара Куанбековна
omarova.1999@mail.ru
Студентка факультета международных отношений ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – Г.Ж.Кенжалина

По мере того как продолжают развиваться информационно-коммуникационные технологии (ИКТ), развиваются возможности и проблемы, связанные с ними. Мы находимся на перепутье, когда человечество переходит от общества уже переплетенного с Интернетом к будущему веку автоматизации, BigData (большого количества данных) и InternetofThings (Интернету вещей). Динамичное развитие ИКТ и интернета не знает границ и, как следствие, оказывает трансформирующее влияние на все сферы общества и государства, включая международную политику и дипломатию, в том числе.

Наиболее широкое развитие получила и виртуальная реальность, представляющая собой, создаваемый техническими средствами мир,и передаваемая человеку через его привычные для восприятия материального мира ощущения. Здесь вытекает такое понятие, как *киберпространство*. Именно оно является виртуальной реальностью, представляющей ноосферу, второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей.

Киберпространство имеет существенное отличие от наземного, морского, воздушного и космического пространств: оно создано не природой, а является искусственной конструкцией, имеющей компоненты, которые могут меняться с течением времени [1].

В нынешнем мире быстрый подъем различноговида киберугроз создает весьма важную проблему обеспечения информационной безопасности.В свою очередь киберугроза – это противозаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения социальных, политических или иных целей.Киберугрозыспособны влиять на информационное пространство компьютера, в котором находятся данные, хранятся материалы физического либо виртуального устройства.В наше время все без исключения киберугрозы принято разделять на внутренние и внешние. Причины и источники внешних угроз находятся вне компьютеров компании, как правило, вовсемирной сети. Внутренние угрозы зависят исключительно от программного обеспечения и оборудования, а также персонала компании. Вирусы, спам, удаленный взлом, фишинг, DoS/DDoS-атаки, хищение мобильных устройств относят к внешним угрозам.Например, вирусы, используя для своих целей трафик, каналы связи, рассылая спам, способны нарушить работоспособность программ и компьютеров, уничтожив данные и файлы. Более опасным вирусом, возникнувшим практически в последнее время, является кибероружие, которое нацелено в некоторых случаях на ликвидацию индустриальной инфраструктуры.В последние несколько лет все более актуальной становится защита от такой внешней угрозы, как хищение мобильных устройств, в памяти которых очень часто хранится в открытом виде важная корпоративная информация: персональные данные клиентов и сотрудников, финансовая документация, электронная переписка, интеллектуальная собственность, а также разного рода пароли и идентификационные данные. Кроме этого, существует еще промышленный шпионаж, кража аппаратного обеспечения, преднамеренное причинение ущерба.

Что касается внутренних угроз, то самую значительную угрозу в наше время представляют уязвимости программного обеспечения. Программы пишутся людьми, а им, как известно, свойственно ошибаться. Недоработки и ошибки в наиболее известных программах позже обнаруживают хакеры, и именно эти ошибки ложатся в основу большинства вирусов, троянских программ, червей, которые проникают через эти лазейки в компьютеры.

С началом технологического прогресса истории стали создаваться новые возможности, но всегда найдутся и те, кто использует данные возможности в корыстных целях. Несмотря на угрозу вирусов и вредоносных программ, люди были уверенны в том, что их данные в компьютерных системах безопасны и неприкосновенны. Однако это было до тех пор, пока не произошел взрывной рост воздействия машин в Интернете, которые обеспечили настоящую площадку для хакеров, идущих на различные преступления: кражи данных, совершение мошенничества, взлом засекреченных документов, файлов и т.п. Именно это получило название *киберпреступность*. В связи с этим можно выделить такую яркую личность, какДжулиа́на Пол Ассáнжа , австралийского интернет-журналиста и телеведущего, основателя сайта WikiLeaks. Сайт WikiLeaks представляет собой портал, который вот уже более 10 лет наводняет мир сенсационными расследованиями, секретными материалами, взятыми или украденными в спецслужбах передовых стран. Джулиан Ассанж стал культовой фигурой журналистики, в Америке его называют шпионом и предателем, в других странах – человеком, борющимся за свободу слова. В больших объёмах он обнародовал сверхсекретные материалы о шпионских скандалах, коррупции в высших эшелонах власти, военных преступлениях и тайнах дипломатии великих держав. Не раз он находился под арестом и обвинялся в киберпреступлениях. Инцидент с Эдвардом Сноуденом также является показательным фактом того, насколько интернет-коммуникации и взаимозависимость социальной среды с политикой, экономикой и военным сектором стали важны и влияют на стратегическое планирование лидеров ведущих держав мира. Л. В. Савин утверждает, что если в геополитике уже достаточно разработан научный аппарат и

дефиниции, которыми оперируют политики, эксперты и ученые, то киберпространство в какой-то мере представляет собой «terraincognita», и за обладание этим пространством ведется довольно активная борьба. Крайне показательным является то противостояние, которое заняли в отношении регулирования интернет-пространства различные государства [1].

Совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями, называют кибербезопасностью. Сегодня основными задачами обеспечения безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. Тем самым, кибербезопасность является необходимым условием развития информационного общества, так как кибербезопасность сочетает в себе набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды или киберпространства ресурсов организаций и пользователей. Таким образом, кибербезопасность – это достижение сохранения свойств безопасности, ресурсов организации или пользователей.

В связи с появлением новых технологических разработок начинает развиваться и кибердипломатия в международных отношениях. Благодаря новым технологиям мир, в котором мы живем сегодня, открывает новые возможности и вызовы для дипломатии. С одной стороны, из-за новых и лучших технологий (например, увеличения количества авиаперевозок, роста интернета, мобильных телефонов, социальных сетей) мы теперь можем общаться друг с другом проще и дешевле, чем когда-либо прежде. Мы можем делиться идеями, решать проблемы и поддерживать этот контакт через социальные сети, используя ИКТ. В то же время существуют и проблемы при работе над международной дипломатией, над обеспечением определенной среды и пространства. Например, интернет, веб-сайты, электронная почта и другие социальные сети, в том числе и СМИ, могут предлагать интересные способы поддержания связи между людьми, странами и т.д. Однако существуют серьезные риски при проведении дипломатии через эту среду. Такие проблемы, как информационная война или кибервойна, представляющая собой бескровную, но в то же время смертельную войну, киберпреступность с использованиемкибероружия, предназначенного для нанесения ущерба в киберпространстве, по-прежнему представляют собой реальную угрозу для защиты информации.

Кибердипломатия – это политика национальных государств в области обеспечения международной кибербезопасности и сотрудничество по этому вопросу с другими странами.Именно сотрудничество с другими странами в сфере кибербезопасности способно помочь созданию коллективной киберзащиты. На сегодняшний день сотрудничество стран в установлении мира и стабильности международного сообщества, а также национальной безопасности играет большую роль. Кибердипломатия же представляет эволюцию публичной дипломатии для включения и использования новых платформ коммуникации в XXI веке. Как пояснил Ян Мелиссен в своей работе «Новая публичная дипломатия: мягкая сила в международных отношениях», кибердипломатия «оказывает влияние инноваций в области коммуникации и информационных технологий на дипломатию» [2]. Кибердипломатия также является частью дипломатии: публичной и виртуальной. Основой кибердипломатии является то, что «она признает, что новые коммуникационные технологии открывают новые возможности для взаимодействия с более широкой общественностью путем принятия сетевого подхода и использования большей части все более многоцентровой глобальной взаимозависимой системы» [3].

Под цифровой дипломатией подразумевается использование современных информационно-коммуникационных технологий для реализации дипломатических и сопряженных внешнеполитических задач.В последние годы значение цифровой дипломатии в международной практике неуклонно растет. Наряду с устоявшимися методами работы внешнеполитических ведомств различных стран и традиционными каналами доведения

информации через радио, телевидение и прессу, интернет все шире используется для пропаганды, сбора информации, оказания давления на иностранные правительства, подготовки активистов и стимулирования протестных движений. Основной целью цифровой дипломатии является продвижение внешнеполитических интересов, информационная пропаганда через интернет-телевидение, социальные сети и мобильные телефоны, направленные на массовое сознание общественности и политической элиты [4].

Казахстан, как и любая другая страна, исключительно заимствующая передовые ИКТ, включая технологии обеспечения кибербезопасности, разработанных в других странах, в любой момент может столкнуться с ситуацией, в которой мы выступим в качестве объекта экспериментов или действительной атаки на критически важные объекты информационно-коммуникационной инфраструктуры страны со стороны преступных организаций и отдельных лиц с непредсказуемым результатом.

Для Казахстана ИКТ играют огромную роль в развитии юного государства.

Область автоматизации государственных услуг, рынок электронной коммерции и электронных платежей развивается на принципах обеспечения безопасности личности, общества и государства при использовании ИКТ, а также воплощения деятельности на базе единых стереотипов, обеспечивающих надежность и маневренность объектов информатизации и связи.

Глава государства Н. Назарбаев в своем Послании народу Казахстана от 31 января 2017 года «Третья модернизация Казахстана: Глобальная конкурентоспособность» отметил, что все большую актуальность приобретает борьба с киберпреступностью. В связи с этим Глава государства поручил Правительству создать систему «Киберщит Казахстана», которая будет обеспечивать защиту электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, систему, способствующую устойчивому развитию Республики Казахстан в условиях глобальной конкуренции [5].

Список использованных источников:

1. Л. В. Савин. Кибергеополитика// журнал: «РоднаяЛадога».Москва.2013.С.1
2. Melissen, Jan. Palgrave Macmillan// «The New Public Diplomacy:Soft Power in International Relations».2007. USA. P. 30
3. Melissen, Jan. Palgrave Macmillan// «The New Public Diplomacy:Soft Power in International Relations».2007.USA.P. 57
4. А. Крикунов. Центр анализа террористических угроз // «Цифровая дипломатия и ее значение в международной практике».Москва.2015.С.1
5. Д. Досымбеков// «Киберщит Казахстана». Казахстан.2017.С 1

УДК 327.3.2

ТЕНЕВАЯ ЭКОНОМИКА:ПРОБЛЕМА ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА.

Рахимжанова Элина Рашидовна
elinarakh@gmail.com
Студент 1 курса, специальности 5В020200 - Международные отношения ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – к.п.н., доцент А.Ж.Турханова

В начале 1970-х газета “TheGuardian” впервые применила термин «отмывание денег» вследствие расследования незаконного финансирования избирательной кампании (37 президента США) Ричарда Никсона.Отмывание денег является незаконной деятельностью,спомощью которой легализируются преступные доходы. Многим финансовым трансакциям характерен «след», который привязывает сумму к определенному